B/IFW

CONFIRMATION NO. 6758
DATE OF NOTICE OF ALLOWANCE: June 15, 2005
SERIAL NO. 09/315,628

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	Bjorn Markus Jakobsson
Case:	15
Serial No.:	09/315,628
Filing Date:	May 20, 1999
Group:	2134
Examiner:	Michael J. Simitoski

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: /Bencidenni/ Date: June 28, 2005

Title: Verification of Correct Exponentiation or Other Operations in Cryptographic Applications

---

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following remarks are submitted in response to the Examiner's Statement of Reasons for Allowance (hereinafter "Statement") included in the Notice of Allowability dated June 15, 2005 in the above-identified application.

REMARKS

Applicant has reviewed the Statement as given on pages 2-3 of the Notice of Allowability. Based on this review, it appears that certain portions of the Statement may be viewed as mischaracterizing the actual limitations of the allowed claims.

By way of example, with regard to claim 1, the Statement at page 2, second-to-last paragraph, indicates that the prior art fails to teach or suggest "generating information representative

of first and second proofs . . . ." However, claim 1 actually calls for "generating at least one signal corresponding to information representative of first and second proofs . . . ."

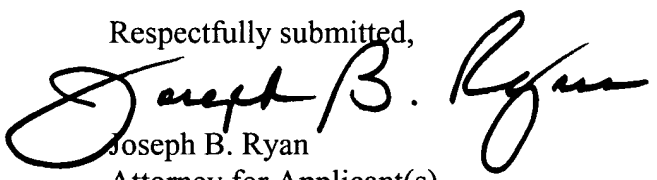
As another example, with regard to claims 23 and 24, the Statement at page 2, last paragraph, to page 3, first paragraph, indicates that the prior art fails to teach or suggest "a transformation protocol which produces a pair (*G*, *Y*) . . . and generates a digital signature using (*G*, *Y*)." This seems to suggest that the digital signature generation is part of the key transformation protocol, which is not the case in claims 23 and 24.

Accordingly, Applicant respectfully submits that the Examiner, in attempting to paraphrase the claimed invention, has introduced language into the Statement that does not accurately reflect the actual claim language.

Also, the Statement characterizes certain prior art references in a manner which is believed to be inconsistent with the positions of Applicant as presented in previous responses. For example, the Statement indicates that the Menezes reference teaches first and second proofs, where the first proof is a proof that an operation has been correctly performed, and the second proof is a proof that the first proof has been correctly performed. Applicant respectfully disagrees with this characterization of Menezes, for the reasons set forth by Applicant in the responses filed April 13, 2004 and September 22, 2004.

Applicant believes that each of the claims is allowable because the particular limitations thereof are not taught or suggested by the art of record. To the extent that the Statement includes language which deviates from the actual language used in the particular limitations of these claims, or language which characterizes the prior art in a manner inconsistent with the positions of Applicant, the Statement is respectfully traversed.

Respectfully submitted,



Date: June 28, 2005

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517